

## **C.1 PURPOSE**

The purpose of this TO is to provide the Joint Improvised-Threat Defeat Organization (JIDO) with Enterprise Information Technology (IT) Operations and Maintenance (O&M) and support services to JIDO Mission IT capabilities.

## **C.2 BACKGROUND**

The Joint Improvised Explosive Device Defeat Organization (JIEDDO) was established in 2006 as a Deputy Secretary of Defense (DSD) directed initiative with the mission to rapidly provide solutions to defeat the enemy's improvised threat campaign and save the lives of service members deployed fighting insurgent networks that employ improvised threats as a strategic weapon of choice. On March 11, 2015, the DSD directed the establishment of JIEDDO as a Defense Agency, designated it as a Combat Support Agency (CSA), and that it be aligned under the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)). On April 30, 2015, the DSD approved an USD (AT&L) request to rename JIEDDO as the Joint Improvised-Threat Defeat Agency (JIDA). JIDA Initial Operational Capability (IOC) occurred October 2015. Subsequently in accordance with Fiscal Year (FY) 2016 National Defense Authorization Act (NDAA) language, JIDA was directed to realign to an existing Combat Support Agency. JIDA began coordination efforts to align with the Defense Threat Reduction Agency (DTRA).

On February 10, 2016, the DOD Resource Management Decision (RMD Number 700A2) for the FY 2017 Presidential Budget was submitted, which implemented the DSD decision to rename JIDA as the Joint Improvised-threat Defeat Organization (JIDO), directed organizational realignment from the Army to USD (AT&L), and approved the request from USA (AT&L) to transfer current JIDA resources from the Services to the JIDO within DTRA and under the authority, direction, and control of the Director DTRA, effective 1 October 2016. On 14 June 2016, USD (AT&L) approved the JIDO Concept of Operations (CONOP), which states (in part), "JIDO accomplishes its mission by sustaining advanced information technology and fusion infrastructure that enables a threat awareness and understanding capability."

Historically, JIDO services support contracts were independently created and implemented by the three organizational entities listed below.

1. Former Counter- Improvised Explosive Device (C-IED) Operations/Intelligence Integration Center (COIC) employed an enterprise strategy entitled "Capstone" supported by GSA Federal Systems Integration and Management Center (FEDSIM) Assisted Acquisition Services (AAS).
2. JIDA Center of Excellence (JCoE).
3. JIDA Contracts Division (CD) solicited and awarded contracts as needed using both internal and external contract acquisition organizations.

In order to streamline and simplify the acquisition of contract support services, JIDO integrated these independent and uncoordinated contracting activities and artifacts into a new Enterprise Acquisition Strategy Initiative (EASI) consisting of six TOs. The overall objectives of the EASI strategy, including this TO, are to:

1. Meet current and evolving mission requirements,

2. Comply with acquisition laws, regulations, and policies.
3. Improve mission effectiveness, output, and organizational synergy.

JIDO enables DoD actions to counter improvised threats in support of Combatant Commanders with tactical responsiveness and anticipatory acquisition to prepare for and react to battlefield or operational surprise. JIDO is an integrated joint organization that supports counter-terrorism (CT), counter-insurgency (COIN), and other related mission areas including C-IED. JIDO responds to changing threats where improvised weapons and associated threat networks are having the most adverse effects on United States (U.S.) Joint Force maneuverability and force protection.

This TO provides direct support to the JIDO J6 organization. The J6's mission is to enable rapid aggregation, fusion, and dissemination of operational information, intelligence, and technology to respond to emerging threats. The J6 organization solves emerging analytical problems through implementation of custom-developed IT capabilities as well as by operationalizing advanced technologies from public, private, and academic sectors. The J6 rapidly responds to Mission Partner Requests for Support (RFS) and enables IT elements of JIDO's mission.

The J6 Enterprise IT Operations (EITO) division is the IT support provider for the JIDO mission enclave, which is the enterprise networks, IT infrastructure, and IT services that support JIDO users and mission capabilities. EITO provides IT O&M and enables the path to production for JIDO Mission IT capabilities, leverages DoD and Intelligence Community (IC) enterprise services, and delivers IT capabilities in response to Mission Partner RFS. JIDO's mission support requirements will evolve as the organization aligns with DTRA. As a result, JIDO requires a highly collaborative and adaptive Industry Partner that will adapt and scale (i.e., increase, decrease, optimize, etc.) level of effort and capabilities as JIDO's mission evolves. Throughout the course of this TO, implementation of shared or hybrid service models with DoD, IC, and DTRA service providers will be required.

### **C.2.1 CURRENT INFORMATION TECHNOLOGY ENVIRONMENT**

EITO serves as JIDO's centralized IT and Mission IT capability support organization, providing local and remote support to JIDO operations around the globe. EITO provides a globally connected infrastructure distributed across three primary security/classification domains, special purpose networks, development environments, staging and testing environments, and a data-center to support JIDO's Mission IT capabilities. EITO supports connectivity to partner sites including Combatant Commands (COCOMs) and Theater Special Operations Commands (TSOCs). EITO executes all IT-related, enterprise-wide hardware, software, and support services purchases for JIDO.

EITO currently supports approximately 1,500 users (i.e., 975 base users plus surge users, tenants, and personnel from other Government agencies who operate on JIDO domains) at two facilities in Northern Virginia (Reston and Crystal City). All JIDO users require access to unclassified and secret networks. Approximately 70 percent of users require access to the Joint World-Wide Intelligence Communications System (JWICS) and/or IC enterprise desktop services. JIDO's mission enclave infrastructure includes JIDO local area networks and enclaves (e.g., Unclassified, Secret, and Top Secret-Sensitive Compartmented Information (TS-SCI)), connections to DoD and IC enterprise networks, interconnections to remote JIDO CONUS and OCONUS locations, other specialized networks (e.g., USG, allied, coalition, special access

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

networks), and interconnections with the DTRA enterprise. JIDO's Secret Internet Protocol Routing Network (SIPRNet) connected network (SLAN) serves as the primary mission network. JIDO's Unclassified Internet Protocol Router Network (NIPRNet) connected enclave (NLAN) supports administrative functions, internal and external unclassified data communications. JIDO's service desk responds to approximately 20,000 user calls per year and resolves an average of 1,600 support tickets per month.

User types and locations are as follows (in approximate numbers and subject to change):

<b>Users</b>	<b>Quantity</b>
JIDO, Reston, Virginia	1,260
JIDO, Crystal City, Virginia	140
Tenants, Crystal City, Virginia	100

JIDO's IT enterprise is composed of the following IT assets (in approximate numbers and subject to change):

<b>Asset Type</b>	<b>Asset Quantities</b>
Workstations/laptops	3,400
Servers (bare metal)	400
Data Storage	350
Network Infrastructure	500
Infrastructure Security	70
Mobile devices	200
JIDO Expeditionary Kits (JEK)	17
Miscellaneous tracked office automation assets (monitors, printers, copiers, etc.)	3,000

EITO supports JIDO's Mission IT capabilities by enabling mission capability path to production and by providing platform, hosting, O&M, cybersecurity, compliance, change management, and Tier I and II support. EITO personnel collaborate daily with the J6 Mission IT organization to optimize and automate the path to production for mission capabilities. The J6 Mission IT organization has created a one-of-a-kind capability to ingest, fuse, analyze, and present mission-relevant data and information with the potential to provide immediate assistance to DoD and the Whole of Government. This capability is a fully authorized SIPRNet and JWICS hosted data analytics cloud architecture. The architecture allows for data access, system stability, scalability, and advanced analytical capabilities across approximately 600 data sources with more data sources added regularly. Access to comprehensive, timely, and accurate data and information is critical to intelligence analysts to help their leaders make informed decisions. JIDO's capability is a cloud architecture based on the National Security Agency (NSA) Ghost Machine Cloud Reference Architecture. The system's stack is comprised of core technologies primarily from the open-source community (e.g., Apache Accumulo, Solr, Hadoop File System (HDFS), Kettle, etc.).

Complimenting JIDO's data analytics cloud architecture is a suite of tools that leverage the data processing power of the system to rapidly discover information such as people, places, phone

numbers, email addresses, and then search through the data by keyword, time, and location filters. The tools include advanced search and filtering capabilities, Keyhole Markup Language (KML) generators and visualization tools.

### **C.3 SCOPE**

The scope of this TO includes all aspects of JIDO IT support to the mission enclave and enterprise IT customer support and solutions services including: program management, IT purchases (including procurement and management of all licenses and subscriptions for JIDO software and other support), customer services, network engineering, systems engineering, network operations, desktop engineering, cybersecurity, assessments and testing, disaster recovery (DR), support to JIDO Mission IT Capabilities, optimization of Mission IT path to production, and maintaining connectivity to mission-partner networks in the Continental United States (CONUS) and Outside the Continental United States (OCONUS). TO scope includes support to deployed forces and providing IT services in theater as required by world events and mission-partner requirements. TO scope includes DTRA transition support including IT support such as technical exchanges with DTRA.

### **C.4 TASKS**

The following describes the services required for each task. The contractor shall provide products and services in a timely and cost-effective manner and shall perform to or exceed the desired outcomes contained in the Performance Requirements Summary (PRS) in **Section J, Attachment I**.

- a. **Task 1 Provide Program Management:** Program Management includes the effective and efficient management of all contractor work including the accountability and security of all personnel. Program Management ensures that contractor performance is within agreed upon quality, cost, and schedule objectives. Program Management ensures cost-effective acquisition of IT hardware, software, services, and subscriptions. Program Management also supports Government planning and decision processes with cost estimates, technical plans, status reports, performance estimates, and other decision support information.
- b. **Task 2 Provide Transition-In and Transition-Out:** Transition-In ensures the smooth and orderly transition from the current contracts. Transition-Out ensures all knowledge, data, material, and information developed by or provided to the contractor is transitioned and delivered to the Government by the end of the TO.
- c. **Task 3 Provide Mission Enclave Technology Support:** JIDO's mission enclave and associated IT infrastructure deliver mission capabilities and support IT users on multiple domains and classification levels. JIDO capabilities are engineered to meet mission requirements and availability at or above the Operational Availability (Ao) levels defined in the Acceptable Quality Level (AQL) for all JIDO data, networks, and systems and as described in the PRS (**Section J, Attachment I**). Cybersecurity ensures that JIDO's mission enclave is secure, compliant, and authorized in accordance with the requirements of DoD Instruction (DoDI) 8500 series of documents, IC Directives, U.S. Cyber Command (USCYBERCOM) taskings, NSA and Defense Information Systems Agency (DISA) inspections, external audits, etc. Assessment and testing services deliver impartial compliance testing and security-control assessments to support JIDO's

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

cybersecurity officials. Deployed IT capabilities provide complete lifecycle management and support including acquisition, integration, logistics, training, user support, innovation, and telecommunications services in response to RFS from deployed users.

- d. **Task 4 Provide Customer Support Services and Solutions:** Enterprise IT services provide a wide range of direct and automated user support services to aid and assist end users employ the capabilities of the mission enclave and associated Infrastructure to the maximum benefit of the JIDO mission. Customer support services include Service Desk, Direct User Support, Email, Audio-Visual, Mobile Technology, IT Asset Logistics, Telecommunications, Website/Portal, and Technical Documentation.
- e. **Task 5 Provide Additional As Needed Support (Optional Task):** This task provides additional services within the scope of this TO, anywhere in the world, in support of evolving JIDO mission initiative requirements, unforeseen world events, real world emerging threats, Decisive Efforts, etc.
- f. **Task 6 Provide IT Project Support Services (Optional Task):** The contractor shall provide IT technical services in support of JIDO initiatives and mission-enclave technology projects within the scope of this TO.

#### **C.4.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT**

**Desired Outcomes:** the PRS (**Section J, Attachment I**): TO performance is delivered at or above PRS (**Section J, Attachment I**) Acceptable Quality Levels (AQL) for quality, cost, and schedule. JIDO benefits from continuous improvements in effectiveness, efficiencies, and cost savings. Delivery of IT services is effective and responsive to changing mission requirements.

The contractor shall provide all necessary program management and contractor personnel resources necessary for the support of this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this TO.

The contractor shall provide an TO Program Manager (TOPM), by name, to serve as the primary interface with the FEDSIM Contracting Officer's Representative (COR) and JIDO Technical Point of Contact (TPOC) for matters of operational and technical delivery. The contractor TO PM shall be responsible for managing and overseeing the activities of all contractor personnel as well as subcontractor/teaming partner efforts used in the performance of this effort and contained in this TO.

The contractor shall institute and maintain management and quality processes and methodologies that ensure that the highest quality performance is obtained within cost and schedule constraints of the TO. The contractor shall regularly report technical, financial, personnel, and general managerial problems to the FEDSIM COR and JIDO TPOC throughout the TO period of performance, and elevate the immediacy of the reporting based on the significance of the problem. Should the contractor encounter any technical, financial, personnel, or general managerial problems throughout the contract period of performance, the contractor shall immediately contact the FEDSIM COR and JIDO TPOC.

#### **C.4.1.1 SUBTASK 1.1 - CONTRACTOR MANPOWER REPORTING**

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site. The contractor shall completely fill in all required data fields using the following web address: <http://www.ecmra.mil/>.

Reporting inputs will be for the labor executed during the period of performance during each Government FY, which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

The contractor shall provide the Annual Contractor Manpower Report (**Section F, Deliverable 45**) by completely filling in all the information in the format using the following url: <https://cmra.army.mil/>.

As part of its submission, the contractor shall also provide the estimated total cost (if any) incurred to comply with this reporting requirement. Reporting period will be the period of performance, not to exceed 12 months ending September 30 of each Government fiscal year and must be reported by October 31 of each calendar year or at the end of the TO, whichever comes first. Contractors may use XML data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

#### **C.4.1.2 SUBTASK 1.2 – COORDINATE A PROJECT KICK-OFF MEETING**

At the FEDSIM Contracting Officer's (CO) direction, the contractor shall assist in coordinating a TO Kick-Off Meeting within seven calendar days after Project Start at a location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include key contractor personnel, representatives from JIDO J6, the JIDO TPOC, the FEDSIM COR, and the FEDSIM CO. The contractor shall present the following at the Kick-Off meeting:

- a. Transition-In Plan (**Section F, Deliverable 01**), delivered at project kick off
- b. Time Phased Labor Matrix (TPLM) (**Section F, Deliverable 02**), delivered at project kick off
- c. Introduction of TO team members and capabilities
- d. Overview of TO scope, schedule, and deliverables
- e. Security requirements/access procedures
- f. Invoice procedures

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

- g. Points of contact
- h. Additional issues or concerns
- i. Draft Project Management Plan with Quality Control Plan (**Section F, Deliverable 03**), delivered at project kick off

The contractor shall provide a draft copy of the agenda (**Section F, Deliverable 04**) for review and approval by the FEDSIM COR and the JIDO TPOC prior to finalizing. The Government will provide the contractor with the number of participants for the Kick-Off Meeting. The contractor shall provide sufficient copies of the presentation for all attendees.

**C.4.1.3 SUBTASK 1.3 – PREPARE A MONTHLY STATUS REPORT (MSR)**

The contractor shall deliver a Monthly Status Report (MSR) (**Section F, Deliverable 05**) that provides, at a minimum, the following information:

- a. Percentage of funding and ceiling expended per CLIN.
- b. Projected funding exhaustion date per CLIN.
- c. TO overview depicting trending for financial, schedule, staffing, and risks.
- d. Summary of work accomplished by task area and project during the reporting period.
- e. Actual travel costs for the month and planned travel costs for the following month.
- f. A personnel roster in organization chart format of individuals assigned to the TO and whether each is a Full-Time Equivalent (FTE) or a fraction of an FTE. Identify FTE count by task and provide a combined total for the TO. Identify personnel assigned to surge tasks and contributed staffing.
- g. Service Level Agreement (SLA) scorecard depicting monthly performance against AQL for each SLA.
- h. Financial overview by CLIN including actual expenditures, accrued non-invoiced expenditures, graphical representation of current and projected expenditures compared to funded value and ceiling value, and Estimate at Completion (EAC) and Estimate to Complete (ETC) values by CLIN for the current option year.
- i. Invoice and payment history.
- j. Cost, expenditure, and percentage of completion reporting for designated projects, efforts, and initiatives (i.e., tracking of projects designated by the JIDO TPOC or FEDSIM COR for separate project-level tracking and that may be funded with contributed funding, surge funding, or other types of government funding.)
- k. Program issues, risks, and mitigations.
- l. Actions required by the Government.

The contractor shall also deliver a monthly labor CLIN(s) EAC Report that details total estimated costs through the end of the current period of performance (**Section F, Deliverable 06**).

#### **C.4.1.4 SUBTASK 1.4 –PROVIDE TRIP REPORTS**

The contractor shall follow JIDO and FEDSIM travel approval procedures. All travel is to be approved in advance. The contractor shall submit Trip Reports (**Section F, Deliverable 07**) after completion of a trip for all long-distance travel. The Trip Report shall follow guidance and format requirements specified by JIDO and shall include the following information:

- a. Names of personnel who traveled
- b. Dates of travel
- c. Destination(s)
- d. Purpose of Trip (be specific)
- e. Actual Trip Costs
- f. Approval Authority (Copy of the document authorizing travel by JIDO)
- g. Summary of events.

The contractor shall reconcile the Trip Reports with each invoice such that they can be matched month by month.

#### **C.4.1.5 SUBTASK 1.5 – PROVIDE INTEGRATED PROGRAM REVIEWS (IPR)**

The contractor shall present the MSR at a monthly IPR (**Section F Deliverable 08**), to JIDO TPOC and the FEDSIM COR. The IPR shall be scheduled within five business days after MSR delivery, pending availability of Government personnel. IPR materials shall be delivered to the Government at least one working day prior to the IPR date.

#### **C.4.1.6 SUBTASK 1.6 – PREPARE PROJECT MANAGEMENT DOCUMENTATION**

The contractor shall prepare and update, as requested, project management documentation (**Section F, Deliverable 09**) for efforts designated by the JIDO TPOC as IT projects. Project management documentation shall include the following as requested by the Government:

- a. Master project schedule updated and presented monthly, serving as a management dashboard identifying the project lead, short summary description, commit date, initial and revised projected completion dates, percentage complete, funding status, and priority (or other information as approved by the JIDO TPOC).
- b. A one-page “Quad Chart” (or other format as approved by the JIDO TPOC) updated monthly for each individual project, including a short project description, overall status, risk statements including severity (impact and likelihood) and recommended mitigations, next actions, and scheduled milestone(s) status.
- c. Project plans and schedules prepared and updated in Microsoft (MS) Project with work breakdown structures (WBS), milestones, schedules, or other information as appropriate for the project.
- d. Monthly project status presentation to the JIDO TPOC(s) and/or FEDSIM COR, scheduled within five working days of delivery of the Master Schedule deliverable, dependent upon availability of Government personnel and as requested by the Government.



SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

- e. Revised staffing plans and cost estimates that capture changes in level of effort resulting from evolving JIDO mission requirements, IT efficiencies, and/or migration of IT functions to DoD or IC enterprise services.
- f. To support JIDO planning and decision processes, the contractor shall deliver cost estimates, level of effort estimates, staffing plans, project plans, technical approach documentation, and other decision support information. The contractor shall provide project-level tracking (e.g., funds expenditures, EAC, work completion, etc.) for project-based activities as directed by the TPOC.
- g. Track and report JIDO per-seat costs and other measures of JIDO's mission enclave and enterprise IT support costs.

**C.4.1.7 SUBTASK 1.7 – PARTICIPATE IN AND SUPPORT TECHNICAL AND PROJECT MEETINGS**

The contractor shall participate in technical working groups, technical interchange meetings, and program management reviews, and shall support technical requirements review meetings throughout the period of performance in support of JIDO activities. Examples include non-recurring and recurring (on a daily, weekly, or monthly basis) stand-up meetings, IT leadership meetings, project and technical status briefings, requirements reviews, technical exchanges meetings with internal and external organizations, recurring briefings to J6 leadership, and other briefings and meeting support as directed by the JIDO TPOC and/or FEDSIM COR.

The contractor shall be responsible for coordination of IT activities that cross JIDO organizations and for representation on integrated project teams to ensure that JIDA and J6 activities are properly supported by EITO. The contractor shall also develop Briefing/Presentation Materials, Reports, and Plans (**Section F, Deliverable 10**) and communicate TO status and issues to JIDO, FEDSIM, and other stakeholders as appropriate. The contractor shall also prepare a record of each meeting (**Section F, Deliverable 11**), including TO IPRs and status meetings.

**C.4.1.8 SUBTASK 1.8 – PREPARE TECHNICAL REPORTS AND BRIEFINGS**

The contractor shall prepare and update an SLA (**Section F, Deliverable 12**) to augment the PRS for Government review and acceptance. The SLA shall include details on the Performance Measures, AQLs, Monitoring Methods, and Incentives/Deterrents as indicated in the PRS (**Section J, Attachment I**).

The contractor shall prepare Technical Reports and Briefings (**Section F, Deliverable 10**), as directed, related to issues generated during the performance of the requirements of the TO. The reports will be reviewed by the JIDO TPOC and FEDSIM COR and comments will subsequently be provided by the Government, if required. The contractor shall resolve the comments to the satisfaction of the Government and produce updated technical reports.

The contractor shall develop and maintain a Lifecycle Management Plan (LCMP) (**Section F, Deliverable 13**), due no later than June 30 annually. The plan shall make recommendations for refresh of existing hardware, software, and systems and shall identify requirements for new systems and infrastructure upgrades, cost estimates, asset disposal, schedule/timing options, sourcing strategies, or other information as directed by the Government. J6 EITO maintains a lifecycle management plan and is executing an enterprise-wide upgrade of IT infrastructure and network devices in Government FY 2016 and 2017. JIDO requires the contractor to maintain and

execute the LCMP per Government direction and does not require industry partners to propose enterprise-wide upgrades or infrastructure refresh in their initial proposal.

#### **C.4.1.9 SUBTASK 1.9 – CONDUCT PROJECT MEETINGS**

The contractor shall schedule and conduct TO-related meetings as directed. The contractor shall prepare a record of each meeting (**Section F, Deliverable 11**), as directed by the Government.

#### **C.4.1.10 SUBTASK 1.10 – PROVIDE IT ACQUISITION TECHNICAL AND ACCOUNTABILITY SUPPORT**

The contractor shall provide technical and administrative support to the JIDO enterprise pertaining to the purchase of IT hardware, software, and related infrastructure needs. The contractor shall develop and maintain comprehensive project cost estimates, projections, and IT Spend Plans (**Section F, Deliverable 14**). Purchases of IT hardware, software, and specialized services (e.g., mobile devices and phones, wireless services, technology support services, telecommunications, etc.) for the JIDO enterprise will be made through approved contract processes as described in section H.11. Contractor spend plans shall forecast and track new requirements, renewals, supplies (e.g., bench stock and routine maintenance items), and other items as directed by the JIDO TPOC. Contractor spend plans, supporting technical specifications, and purchase requests in JIDO acquisition management systems shall be approved by the JIDO TPOC prior to initiating acquisition. The contractor shall follow JIDO Configuration Management (CM) procedures and coordinate with J6 personnel as directed by the JIDO TPOC. The contractor shall coordinate delivery of equipment from suppliers and JIDO warehouse facilities. The Contractor shall comply with JIDO property accountability activities by ensuring that IT equipment is processed through JIDO's inventory accountability processes prior to being placed in service. For accountable IT equipment, the contractor shall report movement, replacement, and disposition to the J6 hand-receipt holder.

#### **C.4.1.11 SUBTASK 1.11 IMPROVE EFFICIENCIES AND EFFECTIVENESS**

The contractor shall establish a continuous process improvement program with the objective of reducing costs while improving quality and mission effectiveness. Cost reductions that are accompanied with demonstrated quality improvements will be rewarded in accordance with a scheme proposed by the contractor (e.g., earned award fee) and approved by the Government in the PRS and award-fee activities.

The contractor shall identify and propose discrete innovation projects (IPs) for Government approval. Proposed IPs are not restricted to this TO. Each IP shall include the following information as a minimum:

- Estimated cost savings or cost avoidance.
- Expected and measurable improvements to quality or mission effectiveness.
- Time line for implementation.
- Government provided material, information, assistance, and funding.

For each Government approved IP, the contractor shall prepare and submit an implementation plan within 30 calendar days (**Section F, Deliverable 15**). The Government will prioritize the IPs and authorize a start date for each. The contractor shall track and report estimated and

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

actual/realized cost savings or cost avoidance as well as realized quality and mission effectiveness changes (positive or negative) for each Government-approved IP.

**C.4.1.12 SUBTASK 1.12 ASSIST JIDO TRANSITION TO DTRA**

The contractor shall assist JIDO transition to the DTRA in accordance with the Government's Transition Plan. This includes preparing written material for JIDO approval, supporting and participating in meetings between JIDO and DTRA, identifying opportunities for interagency cooperation, teaming, integration, and recommending changes to operating procedures.

**C.4.2 TASK 2 – PROVIDE TRANSITION IN AND TRANSITION OUT**

**Desired Outcomes:** JIDO support is sustained in a controlled and deliberate manner throughout transition with no degradation in capabilities. Transition begins immediately at time of TO award. Initial Operational Capability (IOC) is achieved on or before Project Kickoff meeting. Full Operational Capability (FOC) is achieved as soon as possible but no later than 30 calendar days (CONUS-based tasks, as applicable), or 45 calendar days (OCONUS-based tasks, as applicable), after TO award. Transition Out is planned and managed to ensure no degradation in capabilities.

IOC is defined as follows:

1. All required staffing to accomplish transition activities are in place.
2. The initial baseline Transition-In Plan and TPLM, as specified in subtasks 1.2 and 2.1, have been submitted to the Government and required staffing in-processing activities are in progress.
3. Coordination efforts are established and synchronized with legacy contractors for their transition out activities (facilitated by Government).
4. Contractor is in full control of transition activities and required JIDO support is being effectively managed.

FOC is defined as follows:

1. All tasks are fully staffed with fully qualified and trained personnel.
2. Contractor assumes full responsibility for management of all TO requirements.
3. All TO performance measures are in force and enforced.
4. No further support required from the outgoing contractors.

TO staffing shall be phased in over time as world events drive the need for optional, as-needed surge support. Staffing and transition flexibility is the key to successful implementation of this TO. The contractor shall ensure a smooth and orderly transition-in to establish required support, and the contractor shall ensure all knowledge, data, material, and information developed by or provided to the contractor is transitioned and delivered to the Government by the end of the contract period. Historical staffing levels are provided for reference in **Section J, Attachment B**.

**C.4.2.1 SUBTASK 2.1 – IMPLEMENT TRANSITION-IN PLAN**

The contractor shall ensure a smooth transition of support services with no degradation in capabilities during transition. Transition shall begin immediately at time of TO award.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

The contractor shall submit its Transition-In Plan and TPLM on or before project kickoff for Government approval. The Transition-In Plan shall include measurable milestones and decision gates (with entrance and exit criteria) for Government review at weekly Operational Readiness Reviews (ORRs). The TPLM shall identify all personnel and positions to transition to the TO, when they transfer, and their role. The Government will review and accept this TPLM as the initial baseline. Within one week after Government acceptance of the baseline TPLM, the contractor shall ensure the JMD update submission recommendations to the J1 are error-free and continue to follow up and escalate discrepancies reflected in the Government-maintained JMD tool such that it accurately reflects contractor staffing. The contractor shall not invoice before personnel are entered in the JMD. Changes to the JMD must be approved by the JIDO TPOC.

**C.4.2.2 SUBTASK 2.2 - PROVIDE TRANSITION-OUT SUPPORT**

The contractor shall develop a Transition-Out Plan (**Section F, Deliverable 16**) for transitioning and delivering all material and information from this TO to the Government. The Transition-Out Plan shall identify all Government-Furnished and Contractor-Furnished Material (GFM/CFM) as well as information and material developed during the TO that was used in the execution of this TO. The Transition-Out Plan shall be submitted for Government approval. Upon incorporation of comments and Government acceptance, the contractor shall follow the Transition-Out Plan to transfer all material, information, and rights thereto to the Government.

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor and/or Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan NLT 90 calendar days prior to expiration of the TO.

The contractor shall facilitate and conduct transition-out activities. The contractor shall update system descriptions and technical descriptions of all software, systems, and mission support activities delivered or performed under this TO. The contractor shall support transition of administrative and privileged access to the incoming contractor, ensuring that no administrative access is lost. The contractor shall prepare a final report documenting the status of all ongoing efforts and projects (**Section F, Deliverable 10**) and a smart book/turnover binder containing copies of all plans, policies, procedures, points of contact, file storage locations for technical diagrams and documentation, and other information requested by the Government (**Section F, Deliverable 17**). Transition-out shall ensure no disruption to vital Government business. The contractor shall provide full cooperation in providing necessary operational knowledge to the incoming contractor.

Transition-out shall include the following types of services:

- a. Project management processes
- b. Identification of points of contact
- c. Location of technical and project management documentation
- d. Status of ongoing technical initiatives and projects
- e. Incumbent contractor coordination to ensure a seamless transition
- f. Transition of Key Personnel
- g. Identification of schedules and milestones

- h. Identification of actions required of the Government
- i. Establishment and maintenance of effective communication with the incoming contractor and Government personnel for the period of the transition via weekly status meetings

#### **C.4.3 TASK 3 – PROVIDE MISSION ENCLAVE TECHNOLOGY SUPPORT**

**Desired Outcomes:** JIDO mission capabilities and core IT services are delivered at or above the AQL as described in the PRS (**Section J, Attachment I**). Mission enclave technology support services effectively enable delivery of mission capabilities to JIDO internal mission functions and external mission partners in compliance with emerging mission requirements, Government direction, and DoD and IC requirements. The JIDO IT mission enclave is secure, compliant, and available to authorized users 24 hours per day, seven days per week (24x7). The path to the production environment for mission capabilities is continuously optimized to accelerate delivery of capability to users and warfighters. Deployed capabilities are integrated, delivered and supported to meet the mission, functional and schedule requirements of deployed forces. JIDO's mission benefits from innovation and effective implementation of advanced technologies and methodologies.

##### **C.4.3.1 SUBTASK 3.1 - PROVIDE MISSION ENCLAVE ARCHITECTURE AND ENGINEERING SUPPORT**

The contractor shall provide mission enclave infrastructure-related architecture and engineering support and shall provide a Key Personnel lead architect. Support may require local and non-local travel.

The contractor shall be responsible for:

- a. Infrastructure related architecture, engineering, and security architecture.
- b. Ensuring that JIDO's mission enclave infrastructure is optimized to support Mission IT Capabilities and is aligned with JIDO Concept of Operations (CONOPS) to effectively address emerging mission requirements.
- c. Design and engineering of JIDO's IT infrastructure to eliminate single points of failure, to optimize quality of service, and to maximize availability of capabilities to JIDO internal and external users.
- d. IT architecture and engineering for mission enclave DR, Continuity of Operations (COOP), and service availability.
- e. Planning, development, rationalization, and communication of JIDO's mission enclave and enterprise IT technical strategy.
- f. Leading special technology projects (e.g., advanced technology evaluations, proofs of concept, implementation planning) directed by the JIDO TPOC.
- g. Providing technical support to J6 engagements, technical exchanges, product demonstrations, conferences, capability overviews, and briefings internally within JIDO and externally to JIDO partners.
- h. Supporting meetings, delivering briefings, and providing demonstrations to Senior Executives and Flag Officers.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

- i. Providing technical advice and engineering guidance for next-generation planning efforts, including integration or federation with other DoD enterprises and enterprise services.
- j. Preparing briefing materials (**Section F, Deliverable 10**), CONOPS (**Section F, Deliverable 18**), roadmaps and technology plans (**Section F, Deliverable 19**), and other technical materials including DoD Architecture Framework artifacts (**Section F, Deliverable 20**) as directed by the JIDO TPOC.

**C.4.3.1.1 SUBTASK 3.1.1 – MISSION ENCLAVE ENGINEERING SUPPORT**

The contractor shall improve system and infrastructure efficiency and effectiveness through engineering support services, including:

- a. The contractor shall perform system and network engineering. Examples include:
  - i. Implementation of technology to support DevOps enabled capability delivery.
  - ii. Engineering and re-engineering infrastructure due to reorganization.
  - iii. Capability federation and connection to DTRA.
  - iv. Replicating or migrating JIDO Mission IT capabilities, data, and network services to other locations or domains.
- b. Plan and implement transition from internally hosted IT services and mission capabilities to DISA, DTRA, or IC enterprise services or hosting sites as directed by the JIDO TPOC.
- c. Design, engineer, and support data replication to local and remote DR systems.
- d. Plan, pilot, and/or implement mission capabilities and transition to enterprise services, virtualized and cloud-based technologies. JIDO is continually assessing options to transition IT services to cloud-based solutions in compliance with DoD mandates, DTRA transition activities, or to achieve performance efficiencies and improvements. JIDO requires the contractor to support internally-hosted advanced technologies and to support Government decision to transition to enterprise services, but does not initially require the contractor to propose migration of JIDO IT services to a new hosting service or technology stack.
- e. Make recommendations for innovations and improvements in JIDO's mission enclaves that may result in increased efficiency, improved services, and/or reduced costs to the Government.
- f. Provide the following technical reports as requested by the Government regarding the current and projected health of the JIDO IT Infrastructure:
  - i. Plans and procedures for anticipated events such as power outages, weather events, organizational changes, and data calls from Government leadership (**Section F, Deliverable 21**).
  - ii. Trend analysis, incident reports, problem reports, and outage notifications (**Section F, Deliverable 22**).
  - iii. Recommendations, technical proposals, technology roadmaps, and concept planning for improvements and changes for the mission enclave (**Section F, Deliverable 23**).

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

- iv. Mission Enclave Descriptive Documentation delivered annually no later than 30 June (**Section F, Deliverable 24**) that documents and summarizes the architecture, topology, connectivity, and device composition and count of JIDO's infrastructure.

JIDO requires the Contractor to support internally-hosted services and to support transition to enterprise services as directed by the Government, but does not require the Contractor to propose, at time of award, migration of specific JIDO IT services to cloud-based or enterprise services.

**C.4.3.1.2 SUBTASK 3.1.2 CONTINUITY OF OPERATIONS (COOP) AND DR IT SUPPORT**

The contractor shall provide IT support to JIDO COOP and DR efforts and site(s), performing services locally at JIDO, via remote connection to COOP and DR sites, and local travel to remote sites as requested by the Government. Long-distance travel to and on-site services at remote sites may also be required to support JIDO DR and COOP emerging requirements. The contractor shall develop and execute Plans and Procedures (**Section F, Deliverable 21**), as directed by the Government, for JIDO DR capabilities. These plans will be exercised periodically to ensure that safeguards, backups, end-user services, and procedures can provide continuity of mission support services through issues such as natural disasters, power outages, building loss and allow successful recovery of all services after facility restoration or the establishment of alternate facility.

The contractor shall provide the following DR-related services as directed by the Government:

- a. Provide technical support to JIDO DR meetings.
- b. Support technical assessment and perform site surveys for DR candidate sites and hosting services in support of Government planning activities.
- c. Produce written Plans, Designs, Surveys, and Briefings (**Schedule F, Deliverable 10**) to assist JIDO in developing and documenting DR capabilities.
- d. Provide IT technical liaison and coordination with DR facility service providers. Given the interdependence of IT components, collaboration is required and is an important objective.
- e. Support and administer network connectivity, cryptography, circuits, and other communications systems between JIDO and DR facilities.
- f. Provide IT-related technical support to the operation of JIDO DR capabilities.
- g. Support implementation, configuration, and administration of DR systems (virtual and/or physical) that fall within JIDO's IT management control, authorization boundaries, and/or operate as an extension of the JIDO enterprise.

The contractor shall provide the following COOP-related services as directed by the Government:

- a. Provide IT related technical input to JIDO COOP planning, design, and implementation efforts, including meeting and briefing support.

- b. Provide IT related technical liaison, coordination, and Tier I/II support with COOP facility service providers.
- c. Support and administer network connectivity, cryptography, circuits, and other communications systems between JIDO and COOP facilities.
- d. Support implementation, configuration, and O&M of JIDO systems, services, and mission capabilities for COOP IT assets that fall within JIDO's management control, security boundaries, and/or operate as an extension of the JIDO enterprise.

#### **C.4.3.1.3 SUBTASK 3.1.3 PROOF OF CONCEPT, PROTOTYPING, AND PERFORMANCE OPTIMIZATION**

The contractor shall support the J6 mission as an early adopter of innovative technologies and mission capabilities by acquiring, leveraging, and implementing advanced capabilities, methodologies, technologies, and subject matter expertise from public, commercial, and academic sectors that may be conceptual, experimental, or the product of JIDO and non-JIDO Research and Development (R&D) programs. The contractor shall advise Government personnel of relevant new or emerging technologies, perform technology assessments, and provide performance-enhancing recommendations as requested by the Government. Examples include delivery of new Mission IT Capabilities, responses to Mission Partner requests for support, and future alignment of JIDO's mission enclave infrastructure with DoD, IC, or DTRA enterprises.

The contractor shall continuously assess and optimize performance of the mission enclave, including the path and process by which mission capabilities are introduced into JIDO production environments. In collaboration with other J6 organizations (e.g., Mission IT, Capabilities Research Cells, Configuration Management, etc.) the contractor shall optimize and automate the IT capability path to production to accelerate response to mission requirements and delivery of new capabilities. For example, the contractor shall implement and provide O&M of DevOps enabled technologies and capability delivery methodologies.

The deliverables required for this work may take many forms such as Information Papers, Service Catalogues, IT Roadmaps, process and procedure documentation, briefings, training packages, and CONOPS (Section F, Deliverable 18).

#### **C.4.3.2 SUBTASK 3.2 – PROVIDE MISSION ENCLAVE OPERATIONS AND MAINTENANCE**

The contractor shall perform the following work for all JIDO IT infrastructure and systems as directed by the Government:

##### **C.4.3.2.1 SUBTASK 3.2.1 NETWORK AND SYSTEMS OPERATIONS**

- a. Provide installation, configuration, administration, O&M, and operational availability support to JIDO infrastructure, applications, user desktops, and Mission IT Capabilities (e.g., hardware, software, platforms, connectivity, etc.) in testing, staging, and production environments.
- b. Store, back-up, restore, and archive data on all servers and perform recovery operations as needed.
- c. Install, configure, and administer cross-domain solutions, ensuring required separation of



SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

roles and administrative duties.

- d. Maintain and optimize standard configurations, images, and system baselines on all enclave components.
- e. Maintain and administer JIDO's enterprise management tools, such as Solarwinds, Microsoft System Center Configuration Manager (SCCM), System Center Operations Manager, Splunk, etc.
- f. Maintain and operate network and system management software, and other systems such as patch servers, update servers, and storage solutions.
- g. Manage storage systems on all infrastructure components.
- h. Maintain systems hosted for third-party Government organizations in accordance with site licensing agreement, interagency agreements, SLAs, and/or as requested by the Government. Some systems may process data that has restricted access for special access programs requiring read-on by IT personnel.
- i. Provide infrastructure O&M for data feeds and data ingest into Mission IT production systems.
- j. Create and maintain current, written administrative, and system maintenance procedures (**Section F, Deliverable 25**).
- k. Perform acceptance testing to determine suitability of systems and software for operation in the production environment and produce acceptance test reports as requested by the Government (**Schedule F, Deliverable 26**).
- l. Implement cybersecurity corrective actions, patches, bug fixes, and other remediation activities per Plan of Action and Milestone (POA&M) and other requirements to maintain cybersecurity compliance.
- m. Develop, update, and maintain technical documentation, user guides and “how to” materials to assist mission enclave users (**Section F, Deliverable 27**).
- n. Draft IT-related guidance and instructions for incorporation into JIDO Fragmentary Order (FRAGO) issuances. (FRAGOs serve as internal directives that task JIDO J Staffs and organizations with action, coordination, and/or response.)
- o. Install, implement, and integrate systems hosted for third-party organizations in accordance with site licensing agreement, interagency agreements, or as requested by the Government.
- p. Administer, maintain, customize, and optimize JIDO’s implementations of workflow automation solutions that currently include BMC Remedy and Atlassian JIRA.
- q. Support the disposition of obsolete and excess IT equipment by sanitizing and preparing equipment for disposal or transfer to appropriate DoD organizations.

**C.4.3.2.2 INCIDENT, PROBLEM, OUTAGE, AND TROUBLE MANAGEMENT**

- a. The contractor shall notify the JIDO TPOC, verbally or by email if the JIDO TPOC is unavailable, within 15 minutes (or other time period approved by the JIDO TPOC) of confirmation of an outage.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

- b. When diagnosing and troubleshooting service outages, the contractor shall escalate to vendor support upon two hours of on-site resolution attempts or sooner upon confirmation of a product or vendor-specific fault that requires vendor response.
- c. Monitor the mission support infrastructure and capabilities for emerging and actual incidents, problems, outages and other events impacting IT performance and/or cybersecurity status.
- d. Provide preventative mitigations to faults and service degradations where possible through proactive measures to address service degradation or interruption for JIDO users and mission partners.
- e. Provide off-hours remote or call-in support with a two-hour response time for outages to mission capabilities, mission-critical services, infrastructure availability, and JIDO leadership support. Unless otherwise directed by the JIDO TPOC, IT capabilities at COOP/DR facilities shall be considered mission-critical services with a four-hour response time to outages of COOP/DR systems when the primary JIDO facility remains functional.
- f. Prepare After Action Reports (AAR) (**Schedule F, Deliverable 28**) for outages and incidents that degrade or interrupt mission capability services or core services to users. The AAR will describe the incident and identify actions taken, potential future preventative actions, and lessons learned.
- g. Develop or leverage and update/maintain an on-line, automated dashboard showing status of network and system performance, security compliance, and other metrics as requested by the Government (**Schedule F, Deliverable 29**).

**C.4.3.2.3 DATA CENTER OPERATIONS AND MANAGEMENT**

The contractor shall perform the following work:

- a. Design, manage, operate, and maintain the JIDO data center in collaboration with IT engineers and administrators, security personnel, and facilities personnel.
- b. Develop, update, and maintain technical and operational documentation and diagrams. (**Section F, Deliverable 30**).
- c. Support data center expansion, migration, and other changes in response to changing JIDO mission requirements.

**C.4.3.3 SUBTASK 3.3 – CYBERSECURITY SUPPORT SERVICES**

The contractor shall provide cybersecurity services in accordance with DOD 8500 series instructions and other applicable DoD and IC publications, instructions, and TOs. The contractor shall also provide security engineering support and guidance to ensure that the JIDO Mission IT Enclave is compliant with all DoD, IC, DISA and JIDO network security controls, patches, Security Technical Information Guides (STIGS), hot fixes, etc. The contractor shall maintain, track, and report Contractor personnel certifications under DoD Instruction 8570.01 and subsequent revisions. The contractor shall comply with the direction of JIDO cybersecurity officials, including the Authorizing Official (AO), Security Controls Assessor (SCA), and Information Systems Security Manager (ISSM).

Contractor IT activities shall comply with DoD and IC cybersecurity implementation guides, instructions, frameworks, and directives. The contractor shall ensure that cybersecurity requirements are treated like other system requirements and are addressed early and continually throughout the IT lifecycle in response to evolving threat, risk, compliance requirements, and mission.

#### **C.4.3.3.1 SUBTASK 3.3.1 - CYBERSECURITY OPERATIONS**

The contractor shall ensure that JIDO Mission IT enclaves and networks operate in compliance with DoD and IC cybersecurity risk management frameworks, instructions, and directives (e.g., DoDI 8500.01, DoDI 8510.01, IC Directive (ICD) 503, etc.), cybersecurity warning and TOs, and DISA Computer Network Defense (CND) requirements. CND operations will be staffed on site between the hours of 0800 and 1500 on government working days. Additional support hours may be required to support incident response, audits, compliance activities, and specials events directed by the JIDO TPOC to achieve 24 x 7 defense of JIDA IT assets.

The contractor shall perform Cybersecurity services as required, including:

- a. Perform local, onsite CND activities for JIDO Mission IT Enclaves and infrastructure in coordination with the Cybersecurity Service Provider (CSSP) and parent organization cybersecurity functions.
- b. Perform general CND activities for JIDO Mission IT Enclaves and infrastructure.
- c. Provide cybersecurity technical support to patching, remediation, and POA&M activities for JIDO IT infrastructure and production systems throughout the JIDO enterprise.
- d. Serve as Information Systems Security Officers (ISSO) as appointed by the ISSM or AO.
- e. Perform security administration, audit log aggregation, and audit analysis.
- f. Administer and maintain anti-virus, anti-malware, host- and network-based security software, filters, rules, devices, and device-level policies in collaboration with network engineers and system administrators.
- g. Perform incident response, computer emergency response, and support legal investigations and forensic activities.
- h. Maintain cybersecurity related procedures, administrative guides, and technical documentation (**Section F, Deliverable 31**).
- i. Provide Mission IT related security engineering and design guidance support throughout the Software Development Life Cycle.
- j. Support JIDO's implementation of the DevOps path to production and support implementation of automated testing and validation capabilities in collaboration with software developers as directed by the JIDO TPOC.
- k. Provide technical briefings and support to security operations-related meetings with JIDO leadership.
- l. As requested by the Government, conduct threat assessments and produce threat reports as required by JIDO, DoD, and IC instructions and frameworks (**Schedule F, Deliverable 10**).

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

- m. Provide management of JIDO Public Key Infrastructure (PKI) hardware, user tokens, and certificates (e.g., SIPRNet Common Access Cards (CAC), soft or digital certificates for JIDO servers, etc.).
- n. The contractor shall maintain a DISA-compliant registration authority and issue SIPRNet CACs on site between the hours of 0800 and 1700 on Government working days.
- o. Provide security administration and engineering support for guards and cross-domain solutions.
- p. Provide reliable human review for transferring data between systems in accordance with (IAW) JIDO and DoD policies and procedures.
- q. Provide periodic manual and automated data transfer services including cross-domain file transfers, scans, and reviews for the JIDO enterprise in response to user requests and Government direction.
- r. Prevent, detect, and mitigate intrusions.
- s. Provide liaison and coordinate incident responses with the DoD and IC cybersecurity authorities, JIDO's CSSP, and other similar organizations.
- t. Support JIDO emissions security (EmSec) and physical security efforts, including coordination with physical security personnel where appropriate.
- u. Maintain a current list of authorized privileged users, manage authorization and revocation of privileged users, and ensure least-privilege of user accounts and user awareness of security responsibilities (**Section F, Deliverable 32**).
- v. Review and update JIDO user agreements to maintain compliance with evolving DoD and IC requirements (**Section F, Deliverable 33**).
- w. Lead and support efforts for preparation, engagement, and successful outcome of DoD and IC cybersecurity inspections and tests.
- x. Create or leverage and maintain a portal or other automated dashboard to display network and system compliance status and statistics. Where feasible, display compliance status using DoD readiness inspection metrics and other metrics approved by the JIDO TPOC (**Schedule F, Deliverable 29**).

**C.4.3.3.2 SUBTASK 3.3.2 CYBERSECURITY RISK MANAGEMENT SUPPORT**

The contractor shall support JIDO risk management activities including authorizations, risk assessments, and threat assessments in accordance with DoD and IC Risk Management Frameworks (RMF) and processes. The contractor shall draft and staff authorization packages, authorization letters, and other risk management documentation for all JIDO IT assets (e.g., infrastructure, networks, interconnections, commercial software, custom developed applications, systems, and frameworks).

The contractor shall perform security services throughout the IT lifecycle, including:

- a. Ensure that risk management packages are developed and maintained concurrently throughout the system life cycle, beginning at inception of new IT activities.
- b. Comply with and coordinate with JIDO CM processes.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

- c. Support JIDO cybersecurity and risk management officials including the AO, ISSM(s), and SCA as needed.
- d. Execute risk management support and develop packages using processes and templates that are approved by the cognizant risk management official.

The contractor shall perform Risk Management support services as directed by the Government:

- a. Support JIDO's efforts to implement and comply with DoD and IC RMF and legacy Certification and Accreditation (C&A) processes, including transition of systems and networks to the RMF.
- b. Maintain and populate JIDO's instance of the DoD Enterprise Mission Assurance Support Service (eMASS).
- c. Prepare RMF packages, including security plans, system descriptions, diagrams, data flows, POA&M, security assessment reports, and other documentation (**Schedule F, Deliverable 30**).
- d. Update, maintain Certification and Accreditation (C&A) packages that may be required for legacy systems prior to transition to the RMF.
- e. Provide technical support to risk assessments and risk determinations, including preparation of Cybersecurity Impact Assessments (**Schedule F, Deliverable 10**) that summarize test results, risks, and threats in support of ISSM, SCA, and AO risk decisions.
- f. Provide security engineering support throughout RMF IT lifecycles in coordination with system engineers and software developers. Examples include identification of common controls, system categorization, security control selection, security control tailoring, and provide design and implementation guidance to software developers, system engineers, and network engineers.
- g. Review IT system plans, designs, configurations, and architectures for compliance with DoD cybersecurity requirements.
- h. Assist Government cybersecurity officials with design and implementation of RMF workflow, processes, and procedures.
- i. Track cybersecurity related appointments and maintain current appointment letters (e.g., AO, ISSM, ISSO, SCA, etc.) for signature by JIDO cybersecurity officials.
- j. Provide coordination, liaison, and support of cybersecurity related relationships with external partner organizations, including preparation of cybersecurity-related documentation and agreements for interconnections, reciprocity, and JIDO DR and COOP facilities.
- k. Draft and maintain Cyber-Security Policies and Procedures (**Schedule F, Deliverable 31**).
- l. Support the Government's risk management and approval of commercial, third-party, and open-source software.
- m. Support the organization's liaison with DoD and IC cybersecurity organizations and reporting to enterprise tracking and compliance systems.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

- n. Provide technical briefings, meeting support, and status updates related to Cybersecurity and risk management (**Schedule F, Deliverable 10**).
- o. Create or leverage and update/maintain a portal or other form of management dashboard to automate the tracking and reporting of work queue, status, and performance statistics for documentation packages and other risk-management activities (**Schedule F, Deliverable 29**).

**C.4.3.3.3 SUBTASK 3.3.3 – COMMUNICATIONS SECURITY (COMSEC)**

The contractor shall provide a certified COMSEC manager and alternate. The contractor shall acquire, integrate, and test COMSEC equipment and handle COMSEC keys in accordance with Government (i.e., the National Security Agency) COMSEC and key management directives. Support is required to include accountability, issue, operation, destruction, turn in of all COMSEC key material and equipment and supports in re-key operations. The contractor shall identify, report, and support any changes in JIDO's COMSEC account that may result from transition to DTRA.

The contractor shall:

- a. Perform as a COMSEC point of contact and track all actions involving COMSEC management and support the maintenance of COMSEC accounting records.
- b. As requested, prepare reports concerning COMSEC incidents IAW Government regulations and COMSEC maintenance forms, logs, and reports pertaining to COMSEC material accountability (**Section F, Deliverable 34**).
- c. Maintain up-to-date knowledge of the use the Key Management Systems (KMS) and specialized hardware and software programs used to generate and maintain COMSEC material.
- d. Handle daily operational matters based on the knowledge of COMSEC management and using that knowledge to refer inquiries to appropriate personnel.
- e. Provide support on COMSEC matters pertaining to the use of secure communications devices.
- f. Maintain cryptologic equipment in operational condition and coordinate with JIDO J6 IT engineers to address outages resulting from equipment failure, failed re-key transactions, and other issues that can affect network and system availability.

**C.4.3.4 SUBTASK 3.4 – PROVIDE ASSESSMENT AND TESTING SERVICES**

The contractor shall ensure that JIDO mission capabilities and infrastructure, networks, systems, and applications are tested in compliance with JIDO, DTRA, DoD, and IC instructions, directives, frameworks, and standards. The contractor shall support design and implementation of advanced or automated testing capabilities to accelerate delivery of mission capabilities. The contractor shall provide JIDO Government leads with accurate, objective, and impartial verification of the compliance status of the JIDO IT enterprise. The contractor shall ensure that JIDO testing activities are coordinated, planned, and executed as part of IT system lifecycles and projects. The contractor shall provide effective capacity planning and reporting to enable the JIDO TPOC to prioritize tasks and focus testing resources on critical JIDO priorities. The

contractor shall meet or exceed the AQLs for this task as described in the PRS (**Section J, Attachment I**). The test team shall track and report information such as test capacity, queues, priorities, completion status, performance statistics, and schedules by creating or leveraging a portal or other automated reporting capability approved by the JIDO TPOC (**Section F, Deliverable 29**).

#### **C.4.3.4.1 SUBTASK 3.4.1 - PREPARE/MAINTAIN SECURITY ASSESSMENT PLANS AND TEST PLANS**

The contractor shall prepare and maintain assessment and test plans (**Section F, Deliverable 35**), as directed by the Government. The assessment and test plans shall describe the methodology by which the contractor shall execute each type of testing and shall contain information as requested and approved by the SCA and JIDO TPOC. The contractor shall propose efficient methods of maintaining test plans to minimize paperwork and cost.

#### **C.4.3.4.2 SUBTASK 3.4.2 - DEVELOP TEST PROCEDURES**

The contractor shall develop or identify test procedures and test cases (**Schedule F, Deliverable 36**) for each new JIDO software application, widget, system, integration effort, or technology insertion into the mission enclave as requested by the Government. Test procedures shall be in compliance with DoD and IC directives, frameworks, and guides (e.g., DoD Instruction 8500 series, DISA Security Technical Implementation Guides, Security Requirements Guides, etc.) The contractor shall leverage test procedures, security control assessment procedures, and test tools provided or mandated by the DoD, IC, or other Government entity. This includes continuous monitoring methods in compliance with DoD and JIDO direction. When pre-defined test procedures are not available, the contractor shall propose test procedures for SCA approval and for inclusion in the security assessment report. The contractor shall continuously manage and optimize test methodologies and approaches to improve efficiency and reduce costs.

#### **C.4.3.4.3 SUBTASK 3.4.3 - CONDUCT ASSESSMENT AND TESTING ACTIVITIES**

As directed by the JIDO TPOC, the contractor shall execute approved test procedures to validate the implementation of cybersecurity controls and requirements for JIDO IT assets. Testing shall be conducted to support authorizations, re-authorizations, periodic network tests/scans, periodic compliance testing, continuous monitoring, and preparation for readiness inspections and audits as directed. The contractor shall re-test or validate bug fixes and other remediation activities identified in previously completed test activities.

The contractor shall conduct security control assessments (both common/inherited controls and system-specific controls) in compliance with DoD and IC cybersecurity instructions and risk management frameworks. The contractor shall apply, where feasible, test procedures, methodologies, and tools identified by the DoD and the IC (e.g., DoD Instruction 8500 series, DISA STIGs, DISA Security Requirements Guides (SRGs), and DoD's Knowledge Service) The contractor shall support JIDO continuous monitoring and periodic security control assessments. The contractor shall perform testing of cross-domain solutions using approved test plans in coordination with cybersecurity operations personnel.

The contractor shall review and assess software code, review software code scans and assessment reports, and operate software code scanning tools as prescribed by DoD risk management frameworks and technical guides. The contractor shall identify the existence and

causes (where feasible) of deficiencies, vulnerabilities, and other findings within software code.

The contractor shall design, implement, and maintain a test environment on each level of network as directed by the JIDO TPOC and in coordination with the SCA or other Government testing authority. The test environment will be populated with Government-furnished equipment. The contractor shall prepare and update as, as directed by the Government, a Test Environment Design and Management Plan (**Schedule F, Deliverable 37**) for approval by the JIDO TPOC. This plan shall contain information such as the design or architecture of the test environments, required tools, hardware, software, administrative procedures, and the contractor's approach to maintaining test environments.

#### **C.4.3.4.4 SUBTASK 3.4.4 - PREPARE ASSESSMENT AND TEST REPORTS**

The contractor shall prepare reports that capture all tests/assessments and results with content and structure as approved by the SCA and/or the JIDO TPOC. Where feasible, the reports will include technical recommendations for remediation or mitigation of deficiencies. Reports shall include descriptions of deficiencies and their severity to enable risk determinations by the SCA or other personnel. The contractor shall deliver test reports to Government and industry personnel as directed by the JIDO TPOC. The contractor shall provide technical input to the development of POA&Ms, risk assessment activities, remediation planning, and bug-fix planning. The contractor shall, where feasible, leverage automated test reports or the output of automated tools to improve efficiency and minimize paperwork.

As directed by the JIDO TPOC, test reports and artifacts shall be prepared as an addendum to or component of risk management packages, security assessment reports, authorization letters, memoranda, or other documentation packages. Artifacts may include output from automated test tools, code scan reports, screen shots that depict aspects of system configuration and other information requested by Government risk management officials.

#### **C.4.3.5 SUBTASK 3.5 – PROVIDE DEPLOYED IT CAPABILITIES**

The contractor shall provide robust, flexible, secure, and sustained end-to-end Deployed IT Capabilities in response to Government-approved RFS from JIDO mission partners. The contractor shall provide 24 x 7 phone response and remote support to deployed users of JIDO expeditionary capabilities. The contractor shall tailor capabilities to meet the unique mission requirements of each RFS and shall provide logistical support to ensure that capabilities are delivered by the mission-requirement date. The contractor shall support continuous improvement and identify efficiencies for improved capabilities for deployed users. The contractor shall maintain proficiency with Deployed IT Capabilities and knowledge of each system's configuration sufficient to provide step-by-step remote assistance for all aspects of system assembly, connection, operation, problem resolution, and disassembly.

Deployed IT Capabilities include JIDO Expeditionary Kits (JEK) and other capabilities that may be tailored to mission-partner or emerging requirements (e.g. lightweight kits, specialized communications or computing gear, etc.) Deployed IT Capabilities are an extension of the JIDO enterprise that provide a remote, self-contained desktop, Mission IT analytical tool suite, and communications equipment to deployed analysts. Deployed IT Capabilities are designed to operate in austere, remote locations with minimal or no local IT support. These capabilities generally consist of a standardized platform and suite of communications and analytical software tools that are customized to meet the requirements of each operational location and mission



partner. Components may include ruggedized laptops, satellite data and voice equipment, modems, monitors, mobile or satellite phones, Type 1 or Suite B encryption, peripherals, external hard drives, token readers, switches, hubs, transceivers, backpacks, commercial and government software suites, shipping containers, spare parts and miscellaneous items.

#### **C.4.3.5.1 SUBTASK 3.5.1 – DEPLOYED IT CAPABILITY INTEGRATION**

The contractor shall provide support including assembly, integration, O&M, pre-deployment training, logistics, shipping, and Tier II and III technical support and remote user support. The contractor shall track and report status and location of all deployed IT capabilities and associated equipment. The contractor shall provide complete deployed IT capabilities lifecycle management, shall maintain bench stock and spare parts for repairs and kit refurbishment, and shall manage lifecycle replacements for aging or damaged kits.

Deployed IT Capability lifecycle support includes:

- a. Assessing IT infrastructure, mission, operational, communications requirements and unique Tactics, Techniques, and Procedures (TTP) for each Deployed IT Capability deployment location.
- b. Assessing operational readiness and mission worthiness of each Deployed IT Capability. Identify and implement, with Government approval, options to mitigate the risk of equipment failure upon deployment.
- c. Identifying necessary equipment, telecommunications, encryption, and bandwidth requirements and provide cost estimates where required.
- d. Following JIDO CM procedures, prepare Configuration Review Board (CRB) requests, (**Section F, Deliverable 38**), and provide technical support to J6 approval processes.
- e. Integrating all equipment and telecommunications capabilities required to support the mission at the target location. Deployed IT capabilities are built on standard JIDO device images to ensure compatibility and ease of O&M.
- f. Communications services will be provided as Government-Furnished Equipment (GFE) services through directed sources such as DISA, and will be supported by close coordination and cooperation by the contractor.
- g. Supporting RMF activities in collaboration with J6 cybersecurity and IT personnel to ensure Deployed IT Capability compliance, approved software images, authorizations to operate and connect to JIDO enclaves.
- h. Providing design and other documentation (**Section F, Deliverable 30**) necessary to obtain authorization to operate and connect Deployed IT Capabilities to Government networks.

#### **C.4.3.5.2 SUBTASK 3.5.2 - TECHNICAL AND LOGISTICS SUPPORT FOR DEPLOYED IT CAPABILITIES**

The contractor shall perform the following logistics, shipping, and reporting activities:

- a. Prepare a Pre/Post Logistics Plan (**Section F, Deliverable 39**), subject to Government approval, for each deployed IT capability to be deployed.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

- b. Conduct pre-deployment receipt and inspection of all IT equipment, documentation, shipping containers, and other material that will be deployed in support of the JIDO analytical teams.
- c. Perform pre-deployment staging and testing of the JIDO Expeditionary Kit and upgrades, including: conduct a complete inventory of assets being deployed, replenish missing items, interconnect equipment, and run test procedures to ensure the JIDO Expeditionary Kit or upgrade is functional and meets approved contractor-proposed exit criteria and checklists before shipping.
- d. Provide secure/survivable packaging, handling, shipping, transportation and logistics to deliver Deployed IT Capabilities to approved destinations using DoD or commercial shipping methods, as directed by the Government.
- e. Provide remote, reach-back technical support for in-theater receipt, inspection, set-up, and disassembly to ensure the Deployed IT Capability is functional and meets approved acceptance criteria. In-theater support may be required upon Government approval of temporary duty (TDY).
- f. Document all Deployed IT Capability hardware by creating hand receipts and following property control procedures required by JIDO and JIDO's mission partners.
- g. Provide Tier II and Tier III Government-site user technical support from 8 a.m. to 5 p.m. Monday through Friday, excluding Government holidays. The contractor shall provide on-call phone support after hours to deployed users in remote locations, including users operating in potentially austere or hazardous conditions with no local IT or communications support. Contractors shall maintain proficiency with Deployed IT Capabilities and knowledge of each system's configuration sufficient to provide step-by-step remote assistance with all aspects of system assembly, connection, operation, and disassembly.
- h. The contractor shall collaborate with JIDO J6, J2, and watch operations to enable a fully integrated and coordinated user support experience that is easily accessible 24 x 7 for users of Deployed IT Capabilities.
- i. The contractor shall provide capability status reports (e.g., operational readiness, deployment location, shipping status, functional capabilities, training schedules, etc.), inventory, purchase plans, technology roadmaps, and other information to support J6 leadership (**Section F, Deliverable 40**).

**C.4.3.5.3 SUBTASK 3.5.3 - JIDO EXPEDITIONARY KIT TRAINING**

The contractor shall provide hands-on, system-specific training to familiarize users with the assembly, operation, disassembly, and inventory control of Deployed IT Capabilities. The objective of training is to maximize the effectiveness of JIDO's support to the warfighter and to reduce end-user dependence on reach-back support while in remote operating areas. The contractor shall provide training materials, electronic and hard-copy user guides, reach-back support instructions, and other materials to meet mission requirements (**Section F Deliverable 41**).

#### **C.4.3.5.4 SUBTASK 3.5.4 – TELECOMMUNICATIONS, SATELLITE AND MICROWAVE LINE OF SIGHT ENGINEERING SUPPORT**

In support of JIDO Deployed IT Capabilities, the contractor shall procure, design, integrate, support, and maintain wireless, microwave, and satellite and communications capabilities in response to mission requirements. For example, the contractor shall integrate and maintain mobile/portable satellite communications systems to ensure that Deployed IT Capabilities are self-contained to support deployed forces operating in remote locations. The contractor shall provide telecommunications user support and reach-back capabilities. As directed by the Government, the contractor shall acquire satellite communications services.

The contractor shall provide a JIDO Deployed IT Telecommunications and Satellite Requirements Report (**See Section F, Deliverable 42**) which includes cost and functional analysis, assessments, risks, and courses of action to meet deployed or mobile user telecommunication requirements.

#### **C.4.4 TASK 4 – CUSTOMER SUPPORT SERVICES AND SOLUTIONS**

**Desired Outcomes:** JIDO users, mission partners, and warfighters receive highly responsive support services and high-quality IT solutions that result in sustained high customer satisfaction. Resolution of incidents and problems, and responsiveness to emerging mission needs meet or exceed the AQLs for Task 4 as described in the PRS (**Section J, Attachment I**).

The contractor shall provide a wide range of customer services to aid and assist end users employ the capabilities of JIDO's mission enclave to maximize the benefit of the JIDO mission. The contractor shall maintain and report appropriate Task 4 personnel certifications and qualifications under DoDI 8570.01. Customer services and service desk operations shall be based on IT Service Management (ITSM) best practices. The contractor may propose implementation of additional standards, management models, and best practices for approval by the JIDO TPOC.

##### **C.4.4.1 SUBTASK 4.1 –SERVICE DESK SERVICES**

The contractor shall provide IT service desk support in JIDO facilities. The primary service desk is located in JIDO's Reston, Virginia facility and shall operate 24 x 7 with full staffing between the hours of 6 a.m. and 10 p.m. on business days. The service desk shall operate with reduced staffing from 10 p.m. to 6 a.m. and on Government holidays to maintain mission support and ability to respond to JIDO mission partners who operate in other time zones or on a 24 x 7 schedule. A secondary service desk located in JIDO's Crystal City Virginia location shall operate between the hours of 7 a.m. and 5:30 p.m. on Government work days. The contractor is not required to staff JIDO service desks during unplanned closures of the Government facility (e.g., weather closures, etc.).

Increases or reductions in service desk hours of operation, services, and/or level of effort may be implemented after coordination among the contractor, FEDSIM COR, and JIDO TPOC. For example, adjustments may be required in support of emerging JIDO mission requirements, organizational changes, Mission Partner requests for support, or DTRA transition activities. Response to these requirements may result in permanent or limited-duration changes to service desk support.

The Service Desk shall serve as the single, initial contact point for JIDO users across the enterprise to resolve incidents and problems, including mission IT capabilities, computer

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

security, hardware, software, networks, telecommunications, portal and website platforms, audio-visual, system access, and connectivity for all JIDO networks, including JIDO tenants, deployed sites, and analysis teams. As directed by the Government, the contractor shall provide dedicated service-desk and IT-technical support to JIDO tenants (Government and contractors) on site at facilities in Crystal City, Virginia in support of agreements with co-located organizations.

Work activity may include some or all of the following activities.

- a. Open an incident ticket upon receipt of all initial calls and either answer the question, resolve the problem, or forward the problem to the appropriate technical support staff.
- b. Verify accuracy of trouble tickets and validate the nature of problem reported. Only close trouble tickets after the issue/problem has been resolved. Service desk tickets related to portal and website software not operated by the contractor shall be relayed to the appropriate technical support personnel and are not subject to SLA measures for ticket closure or incident and problem resolution.
- c. Monitor, manage, and optimize user call queues and responses to service-desk phone calls.
- d. Resolve service requests to the maximum extent possible using remote support tools such as JIDO's implementation of Bomgar remote support capabilities. Provide touch labor when required.
- e. To the extent feasible resolve customer problems and respond to customer requests while on the telephone with the customer.
- f. Escalate resolution of the problem according to JIDO TPOC-approved escalation procedures. Provide the caller with a realistic estimate of the time required to resolve the problem.
- g. Routinely update and manage assigned trouble tickets. Provide daily ticket queues and Very Important Person (VIP) support status to Government customer service leads via dashboard, email updates, and in person where required.
- h. Establish and maintain accounts and passwords for all infrastructure users and control access.
- i. Confirm with each customer that his or her problem has been resolved and verify customer satisfaction with service provided.
- j. Obtain a customer satisfaction report for each incident, periodically survey users for overall satisfaction, and support third-party or independent user surveys and quality assessments.
- k. Develop procedures, provide technical support, and support service-desk solutions for use of DoD and IC enterprise services, allowing for effective delivery and coordination of local JIDO service desk activities. Interface with the services of the enterprise service provider.
- l. The contractor shall assess the existing self-help capability and improve or re-develop and maintain an automated, on-line, easily accessible, user self-help feature, including a

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

Frequently Asked Questions (FAQ) list, with the intent of reducing the need for users to contact the Service Desk (**Schedule F, Deliverable 43**).

- m. The contractor shall draft, for Government approval, a weekly or bi-weekly newsletter (currently known as the “IT Buzz”) with IT topics of interest, notices, and technical help to users across the JIDO enterprise.

**C.4.4.2 SUBTASK 4.2 - DIRECT USER SUPPORT SERVICES**

The contractor shall provide:

- a. Printer, copier, and fax maintenance (e.g., toner replacement) and repair (break/fix). This includes acquisition of IT commodities, expendables, maintenance and warranty contracts, and supplies to support devices distributed through the facilities.
- b. In collaboration with system and network administrators, provide IT support and customer services for office relocation, including disconnection of existing user equipment, set up, configuration and connectivity, and port activation. The contractor is not required to provide services related to physical transport of equipment.
- c. New employee familiarization and access.
- d. Desk side support to users.
- e. Password set up, reset, and support.
- f. Voicemail setup, reset, and support.
- g. Training and awareness for JIDO IT Infrastructure capabilities, operations, policies, and rules of operation.

**C.4.4.3 SUBTASK 4.3 –EMAIL SERVICES**

The contractor shall provide email services for multiple security levels in support of the JIDO and mission. Specifically, the contractor shall:

- a. Provide Tier I and Tier II support to DoD’s NIPRNet enterprise email services and future migrations to other enterprise services as required. Enterprise email solutions may require support of hybrid solutions comprised of both locally maintained systems and enterprise services.
- b. For SIPRNet and JWICs enterprise email efforts, provide IT planning support, engineering, designs, technical management, coordination, and O&M for migration to and operation of DoD and IC enterprise email services when directed by the JIDO TPOC.
- c. Create and manage email accounts, manage mailbox sizes, and maintain a global active directory that is coordinated with DoD or IC directories.
- d. Provide consistent support and functionality for all JIDO email users regardless of end-user / server operating systems.
- e. Provide remote email access as authorized by the Government and coordinate with DoD mobility capabilities and programs.
- f. Provide virus checking and Spam filtering.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

- g. Coordinate with DoD and IC enterprise cross-domain email services.
- h. Establish, implement, and manage policies concerning naming conventions, distribution lists, send/receive throughput, retention, backup, and data management, in accordance with JIDO and DoD requirements
- i. Develop, update, and maintain technical and operational documentation as well as training materials (**Section F, Deliverable 41**).

**C.4.4.4 SUBTASK 4.4 - AUDIO-VISUAL (AV)/VIDEO TELECONFERENCE (VTC) SUPPORT SERVICES**

The contractor shall provide on-site VTC support services at JIDO's Reston and Crystal City facilities. The contractor shall coordinate and provide technical support for all JIDO AV and VTC systems and facilities. JIDO leadership meetings, inter-agency VTCs, agency-wide all-hands meetings, and other mission-critical meetings generally require both remote and direct, in-person support throughout the duration of the meeting.

The contractor shall ensure that facilities are operated and maintained in accordance with organization security policies and procedures. The contractor shall provide VTC and conference room AV training to Government personnel, such as executive assistants and frequent VTC users. The contractor shall determine AV equipment and VTC facility setup requirements, based on users' needs, system capabilities, and accepted production and presentation techniques.

The contractor shall track and manage (to include purchase after request and Government approval) all AV equipment, software licenses, and maintenance agreements and incorporate AV equipment life cycle planning into the IT O&M LCMP deliverable (**Section F, Deliverable 44**) to ensure that equipment is replaced in a timely and cost-effective manner as requirements emerge or technology improves. The contractor shall also evaluate new technologies and compare to validated requirements, recommend new equipment, configurations, system enhancements, or technological changes that would result in improved system cost effectiveness and/or user productivity. The contractor shall be responsible for installing hardware and software related to conference room AV and VTC facilities and maintaining associated network, computers, peripherals, and audio and/or video equipment. The contractor shall support planning, installation, configuration, and operation of enterprise technologies (e.g., Defense Connect Online, MS Skype, and Tandberg) to improve mission support and to ensure that JIDO achieves maximum value from DoD enterprise solutions. The contractor shall replace equipment IAW LCMP and as directed by the Government. The contractor shall support the following capabilities, including, but not limited to:

- a. Digital video recording
- b. Video Teleconferencing
- c. Knowledge walls, digital white boards
- d. Webcasts
- e. Defense Chat Online (DCO), MS Lync, and other collaborative technologies
- f. Commercial and Government collaboration tools

In addition to providing the above capabilities, the contractor shall:

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

- a. Maintain system reports on utilization, system performance, and maintenance.
- b. Prepare facilities for each individual conference and monitor equipment performance during videoconferences. Identify requirements and maintain a plan to provide direct support to JIDO's command group. Videoconferences are in JIDO facilities and events occur throughout the day. The contractor shall maintain operating procedures for user support.
- c. Determine users' visual aid requirements and ensure that they are produced in the proper format and aspect ratio for transmission.
- d. Review and respond to user requirements for recordings.
- e. Update training programs, as required, to reflect equipment modification, new equipment, or changes in operating procedures.
- f. Develop procedures for and provide direct support to JIDO senior leadership, ensuring complete AV and VTC support and quality of service for the duration of the service request.
- g. To the extent possible, integrate AV and VTC customer support services with JIDO customer services and service desk, providing a centralized service desk capability to track, coordinate, and deploy AV and VTC support.
- h. Establish and maintain standard operating and usage procedures.
- i. Maintain current working knowledge of and implement the latest technological advances in AV, VTC, and other related topics.

**C.4.4.5 SUBTASK 4.5 – MOBILE TECHNOLOGY SERVICES**

Provide worldwide support services for JIDO's mobile end-users. The contractor shall provide access to JIDO infrastructure services for authorized remote users. This includes management, maintenance, and cybersecurity compliance for JIDO's pool of Government-owned mobile equipment. As directed by the Government, the contractor shall acquire and manage commercial wireless data and voice services to support JIDO's mobile users. Device types may include, for example:

- a. Mobile phones and hot spots
- b. Laptop and tablet devices
- c. USB-based or other mobile secure operating environments and Virtual Private Network (VPN) solutions (e.g., Ironkey flash drives, Windows to Go, etc.)
- d. Secret and/or TS mobile capabilities under the DoD Mobility Classified Capability (DMCC)

The contractor is responsible for tracking all JIDO IT devices in TO to perform lifecycle management, maintenance, and user support. The contractor shall coordinate with JIDO asset management activities. The contractor shall maintain devices and support users in compliance with classified and unclassified DoD mobility programs, where applicable.

#### **C.4.4.6 SUBTASK 4.6 - IT ASSET LOGISTICS SERVICES**

The contractor shall comply with JIDO property accountability procedures and shall support JIDO facility and property officers for intake of IT equipment supported within the scope of this TO. The contractor shall provide commercial shipping, receiving, and storage space as approved by the JIDO TPOC and FEDSIM COR. The contractor shall be responsible for the following:

- a. Provide and maintain automated IT asset tracking and management solutions in collaboration with JIDO CM.
- b. Receive IT assets including unpacking, ensuring proper distribution, and completing all required documentation.
- c. Ensure that IT equipment is processed through JIDO's inventory accountability processes prior to being placed in service.
- d. Stage equipment for installation.
- e. For bar-coded IT equipment, the contractor shall report movement, replacement, and disposition to the J6 hand-receipt holder.
- f. Dispose of aging equipment, ensuring that all information has been sanitized in accordance with security regulations.

#### **C.4.4.7 SUBTASK 4.7 - TELECOMMUNICATION OPERATIONS AND MAINTENANCE**

The contractor shall:

- a. Provide a phone to each of the occupants of the JIDO, both Reston and Crystal City locations.
- b. Ensure that a minimum of two contractor personnel are trained and have appropriate system access to administer and maintain each of JIDO's phone systems. Contractor administrative support shall be available during normal business hours to resolve service tickets and to respond to JIDO users.
- c. Maintain the classified and unclassified telecommunications capability in the facility and upgrade the telecommunications per an approved lifecycle management plan.
- d. Provide planning, engineering, implementation, and O&M support, as directed by the Government, to JIDO migration to new or advanced telecommunications solutions such as Voice Over Internet Protocol (VOIP), Secure VOIP, etc. (Currently, JIDO VOIP systems use the G.711 protocol on internal networks and G.729 protocol for bandwidth-constrained networks and connections, such as deployed users.)
- e. Develop, update, and maintain technical and operational documentation as well as training materials (**Section F, Deliverable 41**).

#### **C.4.4.8 SUBTASK 4.8 - PROVIDE WEBSITE/PORTAL, DESIGN, DEVELOPMENT, OPERATIONS, AND MAINTENANCE**

The contractor shall develop, implement, operate, and maintain all JIDO portals as requested by the Government. The contractor shall develop, operate, and maintain an open collaborative portal to access centralized data, collaborate, and share information and improve access to products and



SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

services for DoD, Whole of Government, and U.S. Allied customers. The contractor shall create MS SharePoint sites with JIDO branding utilizing advanced SharePoint features. The contractor shall implement security requirements for DoD and IC portals and provide access to external users as requested. The contractor shall implement applications and content databases according to DISA, DoD, and IC requirements for SharePoint implementation. The contractor shall integrate solutions and support data release to and collaboration with U.S. allies, North Atlantic Treaty Organization (NATO), and other approved users of JIDO portals. The contractor shall coordinate and align activities with the IT activities of other JIDO Government and industry teams.

As directed by the JIDO TPOC, the contractor shall provide portal design, integration, implementation and O&M:

- a. Design, integrate, implement, and administer SharePoint portals and related systems.
- b. Provide continuous improvement processes to each portal to maintain their utility to DoD, IC, JIDO and other users.
- c. Support refresh, redesign, consolidation, migrations, and other efforts to improve operations while reducing operating costs of JIDO portals.

As directed by the JIDO TPOC, the contractor shall provide content management support:

- a. Implement, operate and maintain portal and website instances for JIDO's internally and externally accessible sites for unclassified networks, secret networks, top-secret networks, coalition, allied, and partner networks.
- b. Derive and analyze customer requirements, translating them into web design steps, web page formats, and file and directory structures.
- c. Participate with other staff members in fine tuning data structures and to support information and decision systems.
- d. Implement portal solutions (SharePoint and related applications) on approved IT platforms and baselines provided by JIDO IT operations.
- e. Collaborate with content owners to perform content management and support the continual refresh and maintenance of JIDO portal content.
- f. Integrate identity management and access control solutions as required to authenticate and manage user access to JIDO portals.
- g. Provide portal-related support and administration for other systems of record both internally to JIDO and externally to DoD. These may include, for example, Comprehensive Cost and Requirement System (CCaRS), General Funds Enterprise Business System (GFEBS), Acquisition Tracking and Management System (ATMS), CheckPoint, Action Tracker, mission-specific portals, and other business applications.
- h. Provide application-level administration of web and SharePoint servers and any related applications and features, including web pages and databases. Contractor personnel shall execute and follow JIDO privileged user agreements and follow privilege management efforts enforced by JIDO IT and cybersecurity personnel.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK  
STATEMENT

- i. Develop, implement, and manage data migration strategies to move approved data from file servers and other storage locations to portals.
- j. Develop, implement, and maintain a Metadata storage solution for JIDO Enterprise Information.
- k. Develop and manage a portal LCMP in coordination with JIDO IT and security engineers **(Schedule F, Deliverable 29)**.
- l. Perform portal software updates and upgrades in accordance with the LCMP and cybersecurity requirements.
- m. Plan and execute migration to DoD and IC enterprise services for JIDO portals, content, and related systems in coordination with JIDO enterprise IT objectives.
- n. Provide full Integration with MS Office products (Word, PowerPoint, Excel, Outlook, Project, and Visio) that are heavily used by the JIDO staff.
- o. Support the development of cybersecurity risk management packages and other documentation to satisfy JIDO, DoD, and IC requirements.
- p. Ensure compliance with website and portal-related cybersecurity and technical standards, guidelines, and frameworks for the DoD and IC in collaboration with JIDO security engineers, testers, and risk management officials.
- q. Support planning and implementation of security testing, remediation measures, and POA&M actions, including support to readiness reviews, audits, and other testing activities.
- r. Perform studies and recommend technical architecture, design, and structure of portal infrastructure.
- s. Collect, analyze, and report portal service usage and performance statistics.
- t. Participate in and support technical meetings with Government and industry personnel.
- u. Coordinate portals and related technology with JIDO COOP and DR solutions, ensuring that JIDO portals are accommodated in and compatible with COOP and DR solutions.
- v. Perform unit testing, integration testing, functional testing, and quality control as needed to ensure proper operation of portal systems and functionality.
- w. Perform trouble shooting, debugging, performance analysis, and error correction and resolve functional issues with websites and portals.
- x. Coordinate scheduled and unscheduled outages with JIDO configuration management and service desk personnel and the JIDO TPOC. This includes advanced notice of scheduled outage notifications and reporting of unscheduled outages.

As directed by the JIDO TPOC, the contractor shall provide releasable portal support:

- a. Collect requirements and implement solutions to enable collaboration and data sharing within JIDO portals and websites that meets DISA, DoD, and IC requirements for data sharing with coalitions forces, U.S. allies, NATO, and other approved foreign users.
- b. Implementation of identity management, access controls, and data management solutions to ensure that data access is granted only to authorized personnel.

- c. Coordinate with JIDO Foreign Disclosure Officers, cybersecurity personnel, and other personnel to define release and access policies, document policy, and technical implementation, and enable auditing and other security measures as required.

**C.4.4.8.1 SUBTASK 4.8.1 - WEB/PORTAL APPLICATION DEVELOPMENT AND ENGINEERING**

As directed by the JIDO TPOC, the contractor shall provide web/portal application design and development:

The contractor shall collect requirements from internal and external customers and for development of JIDO business applications and other portal-related applications. The contractor shall plan, design, develop, test, implement, and maintain portal-related applications and systems. The contractor shall support web development using MS Visual Studio, ASP, .NET, Structured Query Language (SQL) and Java and other tools/software as required.

The contractor shall perform the following services as requested by the Government and in direct collaboration with Government technical managers and branch chiefs:

- a. Serve as web applications developer and programmer for JIDO.
- b. Lead the research, development, testing, and integration in the design of web-based applications in the management of enterprise data.
- c. Develop web parts to enhance SharePoint site and site collection functionality and user experience; develop workflows; develop link and merge and aggregate custom views for various data sources; and establish metadata fields with document sets, internal and external content types.
- d. Support development and integration of dashboards and management reporting tools for JIDO IT functions such as cybersecurity, independent testing, network management, project trackers, and other functions that may require portal-based collaboration and reporting capabilities.
- e. Perform studies, requirements gathering, and analysis and recommend technical design and structure of portal applications, systems, and services; serve as web applications developer and programmer for JIDO.
- f. Test, evaluate, and implement new web-based applications.
- g. Resolve and troubleshoot specific and complex issues involved in the design and ongoing support of JIDO websites and portals.
- h. Develop new methods and criteria to document and implement web applications.
- i. Design, develop, troubleshoot, debug, and implement web applications using current technologies.
- j. Study customer requirements, translating them into web design steps, web page formats, and file and directory structures.
- k. Participate with other staff members in fine-tuning data structures to support information and decision systems.

#### **C.4.4.8.2 SUBTASK 4.8.2 - TECHNICAL DOCUMENTATION SUPPORT**

The contractor shall create portal engineering and architecture documentation, user documentation, configuration and restoration plans, development/test/integration process documents and a portal administration guide. Each required document will be submitted to the JIDO TPOC for acceptance and approval for release.

As directed by the JIDO TPOC, the contractor shall:

- a. For each instance of the JIDO portal or website, maintain documentation for system design, architecture, network connectivity, configuration settings, software versions, and custom JIDO/user developed applications (**Schedule F, Deliverable 30**).
- b. Prepare briefing materials, technical reports, roadmaps, implementation plans, risk management package components, and other technical documentation (**Schedule F, Deliverable 10**).
- c. Deliver technical portal user guides, administrative guides, and training materials (**Schedule F, Deliverable 41**).
- d. Document and report test plans, procedures, and results (**Schedule F, Deliverable 26**).
- e. Develop a portal restoration/recovery plan in coordination with JIDO IT engineers and JIDO COOP and DR solutions (**Schedule F, Deliverable 29**).
- f. Document portal-related policies and procedures (**Schedule F, Deliverable 21**).

#### **C.4.5 TASK 5 – PROVIDE ADDITIONAL AS NEEDED SUPPORT (OPTIONAL TASK)**

**Desired Outcomes:** The contractor shall provide the ability to rapidly scale services and capabilities within the scope of this TO in response to emerging or evolving mission requirements locally, globally, and with JIDO mission partners.

Unpredictable world events demand that JIDO maintain the capability to provide additional as needed support in CONUS and OCONUS, including deployment and hazardous duty/combat zones (HD/CZ) anywhere in the world. As directed by the FEDSIM COR and JIDO TPOC, the contractor shall provide additional as needed support within the scope of this TO anywhere in the world and on very short notice (often 30 days or less). Requirements for support may be generated by organizational changes, DTRA transition tasks, new JIDO initiatives, decisive efforts, evolving mission requirements, emerging problem sets, and inter-agency collaboration and support agreements.

Services performed under this task may include any services within the scope of this TO and may be variable in length and level of effort. Additional as needed support may be project-based or result in long-term increase in base level of effort. Support may also require either short-term (up to two months) or longer-term deployments.

The Government will fund additional support CLIN(s) when additional support is required. Additional support may be funded on a per-initiative basis by JIDO's base budget, by Overseas Contingency Operations (OCO) funds, contributions by mission partners, or Congressional or DoD funds that may require separate project-level tracking and reporting under Task 1.6 of the TO.

**C.4.6 TASK 6 – PROVIDE IT PROJECT SUPPORT SERVICES (OPTIONAL TASK)**

As directed by the Government, the contractor shall provide IT technical services in support of JIDO initiatives and mission-enclave technology projects within the scope of this TO. The contractor shall support up to four concurrent teams of five personnel per TO year throughout the period of performance. Each team shall provide IT support services expertise in the areas of telecommunications and COMSEC, desktop and network engineering, system administration and user support, architecture, and cybersecurity, etc.

IT Project support services shall include the following:

- Connection, integration, or federation of JIDO IT capabilities with the DTRA enterprise.
- Migration of internally-hosted services to a Government enterprise service.
- Design, engineering, implementation and O&M of COOP/DR IT solutions.
- Design, engineering, implementation and O&M of JIDO mission-enclave capabilities at alternate data centers or enterprise services through migration or replication.
- Expansion of JIDO mission-enclave capabilities and technologies to additional networks or support expansion of capability on existing networks.
- Expansion of user-support services and solutions to meet emerging mission requirements, to include expanded 24 x 7 user support, supporting additional JIDO or DTRA facilities.
- Providing proofs of concept, prototyping, and implementation of new or advanced IT capabilities, commercial products, and cybersecurity solutions.
- Providing rapid implementation and risk-management support of new IT capabilities.